

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001197054 A**(43) Date of publication of application: **19.07.01**

(51) Int. Cl.

H04L 9/32
G06F 13/00
G06F 17/60
G09C 1/00

(21) Application number: **2000000893**(22) Date of filing: **06.01.00**(71) Applicant: **MITSUBISHI ELECTRIC
SYSTEMWARE CORP**(72) Inventor: **NISHINA KOICHI
NAGASAKA ATSUSHI**

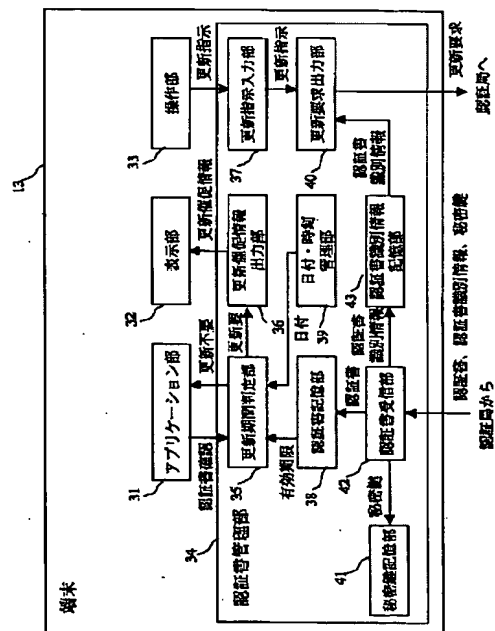
(54) **DEVICE AND METHOD FOR WRITTEN
AUTHENTICATION MANAGEMENT AND
COMPUTER-READABLE RECORDING MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent the validity of a written authentication from expiring, to provide pleasant operability for a user, and to accelerate the smooth operation of a system as to a written authentication management device which manages written authentication.

SOLUTION: An update period decision part 35 decides whether update is needed based on the term of validity included in a written authentication stored in a written authentication storage part 38 and the date managed by a date and time management part 39 and when it is decided that the update is needed, an update urging information output part 36 outputs information urging the update.

COPYRIGHT: (C)2001,JPO



THIS PAGE BLANK (USPTO)

【特許請求の範囲】

【請求項1】 以下の要素を備えることを特徴とする認証書管理装置

- (1) 有効期限を含む認証書を記憶する認証書記憶部
- (2) 日付を管理する日付管理部
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部
- (4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【請求項2】 上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする請求項1記載の認証書管理装置。

【請求項3】 上記認証書管理装置は、認証局と他の認証書管理装置と接続し、上記認証書管理装置は、更に、更新要求を認証局に出力する更新要求出力部と、

更新された認証書を受信する認証書受信部と、受信した認証書を他の認証書管理装置へ送信する要否を確認する情報を出力する認証書送信要否確認情報出力部と、

認証書送信指示を入力する認証書送信指示入力部と、認証書送信指示が入力された場合に、受信した認証書を他の認証書管理装置へ送信する認証書送信部とを有することを特徴する請求項1記載の認証書管理装置。

【請求項4】 認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする認証書管理装置

- (1) 有効期限を含む認証書を記憶する認証書記憶部
- (2) 日付を管理する日付管理部
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部
- (4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【請求項5】 上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする請求項4記載の認証書管理装置。

【請求項6】 上記認証書管理装置は、他の認証書管理装置に接続し、上記認証書管理装置は、更に、更新された認証書を受信する認証書受信部と、更新された認証書が受信された場合に、受信した認証書を他の認証書管理装置に送信する認証書送信部とを備えることを特徴とする請求項4記載の認証書管理装置。

【請求項7】 認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする認証書管理装置

(1) 更新予定日を含む失効リストを記憶する失効リスト記憶部

(2) 日付を管理する日付管理部

(3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部

(4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【請求項8】 上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする請求項7記載の認証書管理装置。

【請求項9】 上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする請求項7記載の認証書管理装置。

【請求項10】 上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする請求項7記載の認証書管理装置。

【請求項11】 認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする認証書管理装置

(1) 更新予定日を含む失効リストを記憶する失効リスト記憶部

(2) 日付を管理する日付管理部

(3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部

(4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【請求項12】 上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする請求項11記載の認証書管理装置。

【請求項13】 上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする請求項11記載の認証書管理装置。

【請求項14】 上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする請求項11記載の認証書管理装置。

【請求項15】 以下の要素を備えることを特徴とする認証書管理方法

(1) 有効期限を含む認証書を記憶する工程

(2) 日付を管理する工程

(3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程

(4) 更新期間であると判定した場合に、更新を催促する情報を出力する工程。

【請求項16】 認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする認証書管理方法

- (1) 有効期限を含む認証書を記憶する工程
- (2) 日付を管理する工程
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程
- (4) 更新期間であると判定した場合に、更新要求を認証局に出力する工程。

【請求項 17】 認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする認証書管理方法

- (1) 更新予定日を含む失効リストを記憶する工程
- (2) 日付を管理する工程
- (3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程
- (4) 更新期間であると判定した場合に、更新要求を認証局に出力する工程。

【請求項 18】 認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする認証書管理方法

- (1) 更新予定日を含む失効リストを記憶する工程
- (2) 日付を管理する工程
- (3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程
- (4) 更新期間であると判定した場合に、更新を催促する情報を出力する工程。

【請求項 19】 以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体

- (1) 有効期限を含む認証書を記憶する処理
- (2) 日付を管理する処理
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理
- (4) 更新期間であると判定した場合に、更新を催促する情報を出力する処理。

【請求項 20】 以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体

- (1) 有効期限を含む認証書を記憶する処理
- (2) 日付を管理する処理
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理
- (4) 更新期間であると判定した場合に、更新要求を認証局に出力する処理。

【請求項 21】 以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体

- (1) 更新予定日を含む失効リストを記憶する処理
- (2) 日付を管理する処理
- (3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理
- (4) 更新期間であると判定した場合に、更新要求を認

10

20

30

40

50

証局に出力する処理。

【請求項 22】 以下の処理をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体

- (1) 更新予定日を含む失効リストを記憶する処理
- (2) 日付を管理する処理
- (3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理
- (4) 更新期間であると判定した場合に、更新を催促する情報を出力する処理。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証書を管理する認証書管理装置に係り、認証書の有効期限切れを未然に防止し、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進する認証書管理装置に関する。

【0002】

【従来の技術】近年、インターネットを介したデータ転送を伴うシステムにおいて、セキュリティの確保の為に、認証局が発行する認証書を用いる方式が一般化している。この認証書には、有効期限が設定されていて、その有効期限を過ぎてしまった場合には、認証局に対して、改めて新しい認証書の発行を要求しなければならず、その手間は煩わしく、システムの円滑な稼動を阻害する。

【0003】また、有効期限内に認証書を更新することによって、継続的にシステムを稼動させることもできるが、認証書の更新の為のオペレーションは、一般のユーザーにとって煩わしいものである。認証書の更新の必要性は、ユーザーに提供するシステムの機能と直接的に関係が無い場合が多い。そのような場合に、ユーザーは、このオペレーションをセキュリティの確保の為に必要な行為であると納得することは出来ず、単に煩雑な印象を与えるものとなる。

【0004】一方、認証書が何らかの理由により、有効でなくなる場合がある。認証局は、このような失効した認証書を一元的に管理し、失効した認証書のリストである失効リストを作成している。システムを構成する端末は、認証局に失効リストを要求し、受信した失効リストに基づいて、失効した認証書の使用を禁止し、認証書の有効性を担保している。しかし、各端末側では、この失効リストを常に最新のものに更新しておかなければならず、更新の為の管理行為は、ユーザーに対して過大な負担を与えている。また、ユーザーが更新を怠った場合には、認証の有効性が保たれないおそれが生じる。

【0005】

【発明が解決しようとする課題】本発明は、上記した従来技術の欠点を除くためになされたものであって、その目的とするところは、認証書の有効期限を過ぎる前に、

ユーザーに認証書の更新を促し、認証書の有効期限切れを未然に防止することである。

【0006】また、認証書の更新手続き自体を、自動化し、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼働を促進する。

【0007】更に、失効リストの更新を自動化し、ユーザーの管理行為の負担を軽減し、併せて失効リストが最新であることを保証し、認証の有効性を担保する。

【0008】

【課題を解決するための手段】本発明に係る認証書管理装置は、以下の要素を備えることを特徴とする。

- (1) 有効期限を含む認証書を記憶する認証書記憶部
- (2) 日付を管理する日付管理部
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部
- (4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【0009】更に、上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする。

【0010】更に、上記認証書管理装置は、認証局と他の認証書管理装置と接続し、上記認証書管理装置は、更に、更新要求を認証局に出力する更新要求出力部と、更新された認証書を受信する認証書受信部と、受信した認証書を他の認証書管理装置へ送信する要否を確認する情報を出力する認証書送信要否確認情報出力部と、認証書送信指示を入力する認証書送信指示入力部と、認証書送信指示が入力された場合に、受信した認証書を他の認証書管理装置へ送信する認証書送信部とを有することを特徴とする。

【0011】本発明に係る認証書管理装置は、認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする。

- (1) 有効期限を含む認証書を記憶する認証書記憶部
- (2) 日付を管理する日付管理部
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する更新期間判定部
- (4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【0012】更に、上記更新期間判定部は、上記日付から上記有効期限までの期間が所定の日数に満たない場合に更新期間であると判定することを特徴とする。

【0013】更に、上記認証書管理装置は、他の認証書管理装置に接続し、上記認証書管理装置は、更に、更新された認証書を受信する認証書受信部と、更新された認証書が受信された場合に、受信した認証書を他の認証書管理装置に送信する認証書送信部とを備えることを特徴とする。

【0014】本発明に係る認証書管理装置は、認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする。

- (1) 更新予定日を含む失効リストを記憶する失効リスト記憶部
- (2) 日付を管理する日付管理部
- (3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部
- (4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新要求を認証局に出力する更新要求出力部。

【0015】更に、上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする。

【0016】上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする。

【0017】上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする。

【0018】本発明に係る認証書管理装置は、認証局に接続する認証書管理装置であって、以下の要素を備えることを特徴とする。

- (1) 更新予定日を含む失効リストを記憶する失効リスト記憶部
- (2) 日付を管理する日付管理部
- (3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する更新期間判定部
- (4) 上記更新期間判定部によって、更新期間であると判定した場合に、更新を催促する情報を出力する更新催促情報出力部。

【0019】上記更新期間判定部は、上記日付が上記更新予定日を過ぎている場合に更新期間であると判定することを特徴とする。

【0020】上記更新期間判定部は、上記日付が上記更新予定日と同日である場合に更新期間であると判定することを特徴とする。

【0021】上記認証書管理装置は、更に、認証局から失効リストを受信する失効リスト受信部を有することを特徴とする。

【0022】本発明に係る認証書管理方法は、以下の要素を備えることを特徴とする。

- (1) 有効期限を含む認証書を記憶する工程
- (2) 日付を管理する工程
- (3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程
- (4) 更新期間であると判定した場合に、更新を催促する情報を出力する工程。

【0023】本発明に係る認証書管理方法は、認証局に接続する装置の認証書管理方法であって、以下の要素を

備えることを特徴とする。

(1) 有効期限を含む認証書を記憶する工程

(2) 日付を管理する工程

(3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する工程

(4) 更新期間であると判定した場合に、更新要求を認証局に出力する工程。

【0024】本発明に係る認証書管理方法は、認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする。

(1) 更新予定日を含む失効リストを記憶する工程

(2) 日付を管理する工程

(3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程

(4) 更新期間であると判定した場合に、更新要求を認証局に出力する工程。

【0025】本発明に係る認証書管理方法は、認証局に接続する装置の認証書管理方法であって、以下の要素を備えることを特徴とする。

(1) 更新予定日を含む失効リストを記憶する工程

(2) 日付を管理する工程

(3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する工程

(4) 更新期間であると判定した場合に、更新を催促する情報を出力する工程。

【0026】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。

(1) 有効期限を含む認証書を記憶する処理

(2) 日付を管理する処理

(3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理

(4) 更新期間であると判定した場合に、更新を催促する情報を出力する処理。

【0027】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。

(1) 有効期限を含む認証書を記憶する処理

(2) 日付を管理する処理

(3) 上記日付と、上記有効期限に基づいて更新期間であるか否かを判定する処理

(4) 更新期間であると判定した場合に、更新要求を認証局に出力する処理。

【0028】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。

(1) 更新予定日を含む失効リストを記憶する処理

(2) 日付を管理する処理

(3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理

(4) 更新期間であると判定した場合に、更新要求を認証局に出力する処理。

【0029】本発明に係るコンピュータ読み取り可能な記録媒体は、以下の処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする。

(1) 更新予定日を含む失効リストを記憶する処理

(2) 日付を管理する処理

(3) 上記日付と、上記更新予定日に基づいて更新期間であるか否かを判定する処理

10 (4) 更新期間であると判定した場合に、更新を催促する情報を出力する処理。

【0030】

【発明の実施の形態】実施の形態1. 以下本発明を図面に示す実施例に基づいて説明する。図1は、本発明におけるシステムの構成図である。13と14は、データの転送を行なう端末である。端末13と端末14は、インターネット11を介して接続されている。また、認証局12と端末13もインターネット11を介して接続されている。認証局12と端末14の間も同様である。

20 【0031】図2は、認証書の構成を示す図である。認証書21には、公開鍵22と、有効期限23が含まれている。この例では、端末13の要求により認証局12が認証書21を発行し、端末13は、認証書21を受信し、更に端末14へ転送する。尚、認証書は、デジタル証明書、デジタルID、証明書、認証証などと呼ばれることもある。

【0032】22は、公開鍵である。公開鍵22は、端末13から端末14へ送られる暗号データを復号するときに用いられる。

30 【0033】23は、有効期限である。有効期限23内においてのみ、認証書21は有効である。従って、端末13側では、有効期限23を超える前に更新の手続きをしなければならない。

【0034】図3は、実施の形態1における端末の構成のうち有効期限の管理に関する部分を示す図である。31は、アプリケーション部、32は、表示部、33は、操作部、34は、認証書管理部、35は、更新期間判定部、36は、更新催促情報出力部、37は、更新指示入力部、38は、認証書記憶部、39は、日付・時刻管理部、40は、更新要求出力部、41は、秘密鍵記憶部、42は、認証書受信部、43は、認証書識別情報記憶部である。

【0035】アプリケーション部31は、データの転送の処理に先立って、認証書の確認を認証書管理部34へ依頼する。

【0036】図4は、実施の形態1における認証書管理部による有効期限の管理の処理フローを示す図である。認証書の確認を依頼された認証書管理部34は、有効期限の管理の処理を開始する。

50 【0037】更新期間判定部35は、認証書記憶部38

から有効期限を読む（S101）。更新期間判定部35は、更に日付・時刻管理部39から日付を読む（S102）。そして、更新する期間に入っているかを判定する（S103）。この例では、有効期限-日付が、予め定められた更新期間に含まれるか否かを判定する。例えば、更新期間が2週間に設定されている場合に、有効期限-日付が13日となれば、更新する期間に入っていると判断する。

【0038】更新する期間に入っていなければ、更新要求出力部40は、アプリケーション部31に更新不要であった旨を通知し、処理を終了する（S104）。

【0039】更新する期間に入っていれば、更新期間判定部35は、更新催促情報出力部36に認証書の更新が必要である旨を伝える。更新催促情報出力部36は、表示部32に認証書の更新を催促する情報を表示させる（S105）。

【0040】ここで、ユーザー15は、続けて認証書を更新するか（これを、更新指示という。）、あるいは、認証書の更新をせずに終了するかを選択し、操作部33を介して入力する。

【0041】更新指示が入力されなかった場合には、処理を終了する。

【0042】更新指示が入力された場合には、更新要求出力部40は、認証局12へ更新要求を送信する。この例では、更新前の認証書識別情報と、ユーザー識別情報を併せて送信する。これによって、認証局12は、新しい秘密鍵と公開鍵を作成し、新しい認証書と、新しい認証書識別情報と、新しい秘密鍵を端末13に送信する。

【0043】認証書受信部42は、新しい認証書と、新しい認証書識別情報と、新しい秘密鍵を受信し（S108）、新しい認証書を認証書記憶部38に、新しい認証書識別情報を認証書識別情報記憶部43に、新しい秘密鍵を秘密鍵記憶部41に記憶させる（S109～S111）。

【0044】続いて、認証書管理部34は、認証書送付の処理を行なう。図5は、実施の形態1における端末の構成のうち認証書送付に関する部分を示す図である。51は、認証書送信要否確認情報出力部、52は、認証書送信指示入力部、53は、認証書送信部である。

【0045】図6は、実施の形態1における認証書管理部による認証書送付の処理フローを示す図である。

【0046】認証書送信要否確認情報出力部51は、表示部32に認証書の送信の要否を確認する表示をさせる。ユーザー15は、この表示により、続けて認証書の送信を行なうか（これを認証書送信指示という。）、あるいは、認証書の送信を行わずに終了させるかを判断し、操作部33に入力する。

【0047】認証書送信指示入力部52に認証書送信指示が入力されなかった場合には（S112）、終了する。

【0048】認証書送信指示入力部52に認証書送信指示が入力された場合には（S112）、認証書記憶部38から新しい認証書を読み（S113）、それを端末14に送信する（S114）。

【0049】認証書管理部34による認証書確認の処理が終了すると、アプリケーション部31は、端末14に対してデータの転送を行なう。このとき、秘密鍵記憶部41に記憶された秘密鍵を用いてデータの暗号化を行なう。

10 【0050】尚、更新要求出力部40から認証局12へ送信される更新要求は、認証局12の方式に依存する。この例では、認証局12から秘密鍵も受信する方法を示した。この場合の鍵の作成は、認証局12が行なうので、更新要求は、更新前の認証書識別情報と、ユーザー識別情報で足りる。一方、端末13で鍵の作成を行なう場合には、認証書管理部34で予め鍵を作成し、作成した秘密鍵を秘密鍵記憶部41に記憶し、更新要求には、更新前の認証書識別情報と、ユーザー識別情報の他に、公開鍵も含める。

20 【0051】また、この実施例では、S101で、更新期間判定部35は、認証書記憶部38から有効期限を読み、S102で、更に日付・時刻管理部39から日付を読み、S103で、更新する期間に入っているかを判定するように構成されている例を示したが、時刻を判定の条件に加えることも有効である。認証書21の中の有効期限23に時刻が含まれ、更新期間が時刻を含めて管理される場合には、更新期間判定部35は、認証書記憶部38から時刻を含めた有効期限を読み、日付・時刻管理部39から現在の日付と時刻を読み、S103で、更新する期間に入っているかを判定する。例えば、更新する期間の長さが48時間で、有効期限が10月10日の午後3時の場合には、10月8日の午後2時は更新する期間外となり、10月8日の午後4時は更新する期間内となる。また、認証書21の中の有効期限23に時刻が含まれていない場合であっても、特定時刻に更新が可能となるときには、更新期間判定部35は、日付・時刻管理部39から日付と時刻を読み、S103で、更新する期間に入っているかを判定する。例えば、認証局による更新処理が午前10（特定時刻）から開始されると仮定し、更新する期間の長さが10日で、有効期限が10月20日の場合に、10月10日の午前9時（特定時刻前）は更新する期間外となり、10月10日の午前11時（特定時刻後）は更新する期間内となる。

【0052】本実施の形態により、認証書の有効期限を過ぎる前に、ユーザーに認証書の更新を促し、認証書の有効期限切れを未然に防止することができる。

【0053】また、ユーザーが認証書の更新の要否を選択できるので、より高い安全性確保のために他の認証書更新方法を採用するなど、柔軟な運用が可能である。

50 【0054】更に、認証書の送信についても、ユーザー

がその要否を選択できるので、同様に他の認証書送付方法を採用するなど、柔軟な運用が可能である。

【0055】実施の形態2. 本実施の形態では、認証書の更新と、認証書の送信を自動的に処理する形態について説明する。

【0056】図7は、実施の形態2における端末の構成を示す図である。更新期間判定部35は、更新指示を直接更新要求出力部40に伝えるように構成されている。また、認証書受信部42が認証書を受信し、認証書記憶部38に認証書が記憶されると、自動的に認証書送信部53が認証書を送信するように構成されている。

【0057】図8は、実施の形態2における認証書管理部の処理フローを示す図である。S101からS103は、実施の形態1と同様である。

【0058】更新期間判定部35が更新する期間に入っていると判断した場合には、更新指示を更新要求出力部40に伝える。更新要求出力部40はこれを受けて更新要求を出力する(S107)。S107からS111は、実施の形態1と同様である。

【0059】認証書送信部53は、S111の処理に続いて認証書を読み(S113)、端末14へ送信する(S114)。

【0060】この例では、認証書の更新と、認証書の送信の両方を自動的に処理する形態について説明したが、一方のみを自動化し、更新催促情報出力部36と更新指示入力部37を付加する構成、あるいは、認証書送信要否確認情報出力部51と認証書送信指示入力部52を付加する構成とすることも有効である。

【0061】本実施の形態により、認証書の更新と、認証書の送信を自動的に処理するので、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼働を促進することができる。

【0062】実施の形態3. 本実施の形態では、失効リストの更新を自動化する形態について説明する。

【0063】図9は、失効リストの構成を示す図である。61は、失効リスト更新日、62は、失効リスト更新予定日、63、64は、失効した認証書の認証書識別情報である。失効リスト更新日61は、この失効リストを更新した日付である。失効リスト更新予定日62は、次に失効リストを更新する予定の日付である。また、失効した認証書の認証書識別情報63、64で識別される認証書は、使用できない。

【0064】図10は、実施の形態3における端末の構成を示す図である。31は、アプリケーション部、34は、認証書管理部、39は、日付・時刻管理部、71は、更新期間判定部、72は、失効リスト記憶部、73は、更新要求出力部である。

【0065】図11は、実施の形態3における認証書管理部の処理フローを示す図である。アプリケーション部31は、動作の開始時等の適当な時期に、失効リストの

確認を認証書管理部34に依頼する。

【0066】更新期間判定部71は、失効リスト記憶部72から失効リスト更新予定日62を読む(S201)。また、日付・時刻管理部39から、日付を読む。そして、両者を比較し、その時点で失効リスト更新予定日62を過ぎていなければ、更新不要の旨を通知し(S204)、処理を終了する。

【0067】一方、比較の結果、その時点で失効リスト更新予定日62を過ぎていれば、更新要求出力部73に対して更新指示を伝え、更新要求出力部73は認証局12へ失効リストの更新要求を出力する。

【0068】失効リスト受信部74は、認証局12から更新された失効リストを受信する(S206)。そして、失効リスト記憶部72で更新された失効リストを記憶する。

【0069】また、この実施例では、更新期間判定部71による比較の結果、その時点で失効リスト更新予定日62を過ぎていれば、更新要求出力部73に対して更新指示を伝える構成を示したが、同日の場合も更新指示を伝えるようにすることも有効である。

【0070】更新期間判定部71の判定の条件に、時刻を加えることも有効である。例えば、失効リスト更新予定日62に更新予定時刻が含まれている場合には、更新期間判定部71は、S201で更新予定日と更新予定時刻を読み、日付・時刻管理部39から、現在の日付と時刻を読み、時刻を含めて両者を比較し、判定する。また、失効リスト更新予定日62に更新予定時刻が含まれていない場合であっても、特定時刻に更新が可能となるときには、更新期間判定部71は、日付・時刻管理部39から日付と時刻を読み、更新する期間に入っているかを判定する。例えば失効リストの更新予定時刻が午後3時と決まっている場合には、更新予定日と同日であっても、午後2時であれば更新予定時刻前であるので更新する期間外となり、午後4時であれば更新予定時刻後であるので更新期間内となる。

【0071】これにより、失効リストの更新を自動化し、ユーザーの管理行為の負担を軽減し、併せて失効リストが最新であることを保証し、認証の有効性を担保することができる。

【0072】実施の形態4. 本実施の形態では、失効リストの更新を催促する形態について説明する。

【0073】図12は、実施の形態4における端末の構成を示す図である。81は、更新催促情報出力部、82は、更新指示入力部である。

【0074】図13は、実施の形態4における認証書管理部の処理フローを示す図である。S201からS203までは、実施の形態3と同様である。

【0075】更新期間判定部71による比較の結果、その時点で失効リスト更新予定日62を過ぎていれば、更新催促情報出力部81に失効リストの更新が必要である

旨を伝える。更新催促情報出力部 81 は、表示部 32 に失効リストの更新を催促する情報を表示させる (S301)。

【0076】ここで、ユーザー 15 は、続けて失効リストを更新するか (これを、更新指示という。)、あるいは、失効リストの更新をせずに終了するかを選択し、操作部 33 を介して入力する (S302)。

【0077】更新指示が入力されなかった場合には、処理を終了する。

【0078】更新指示が入力された場合には、更新要求出力部 73 は、認証局 12 へ更新要求を送信する。これによって、認証局 12 は、新しい失効リストを端末 13 に送信する。S205 以降は、実施の形態 3 と同様である。

【0079】ユーザーが失効リストの更新の要否を選択できるので、より高い安全性確保のために他の失効リスト更新方法を採用するなど、柔軟な運用が可能である。

【0080】

【発明の効果】認証書の有効期限を過ぎる前に、ユーザーに認証書の更新を促し、認証書の有効期限切れを未然に防止することができる。

【0081】ユーザーが認証書の更新の要否を選択できるので、より高い安全性確保のために他の認証書更新方法を採用するなど、柔軟な運用が可能である。

【0082】認証書の送信についても、ユーザーがその要否を選択できるので、同様に他の認証書送付方法を採用するなど、柔軟な運用が可能である。

【0083】認証書の更新と、認証書の送信を自動的に処理するので、ユーザーに対して快適な操作性を提供するとともに、円滑なシステムの稼動を促進することができる。

【0084】失効リストの更新を自動化し、ユーザーの管理行為の負担を軽減し、併せて失効リストが最新であることを保証し、認証の有効性を担保することができる。

【0085】ユーザーが失効リストの更新の要否を選択できるので、より高い安全性確保のために他の失効リスト更新方法を採用するなど、柔軟な運用が可能である。

【図面の簡単な説明】

【図 1】 本発明におけるシステムの構成図である。

【図 2】 認証書の構成を示す図である。

【図 3】 実施の形態 1 における端末の構成のうち有効期限の管理に関する部分を示す図である。

【図 4】 実施の形態 1 における認証書管理部による有効期限の管理の処理フローを示す図である。

【図 5】 実施の形態 1 における端末の構成のうち認証書送付に関する部分を示す図である。

【図 6】 実施の形態 1 における認証書管理部による認証書送付の処理フローを示す図である。

【図 7】 実施の形態 2 における端末の構成を示す図である。

【図 8】 実施の形態 2 における認証書管理部の処理フローを示す図である。

【図 9】 失効リストの構成を示す図である。

【図 10】 実施の形態 3 における端末の構成を示す図である。

【図 11】 実施の形態 3 における認証書管理部の処理フローを示す図である。

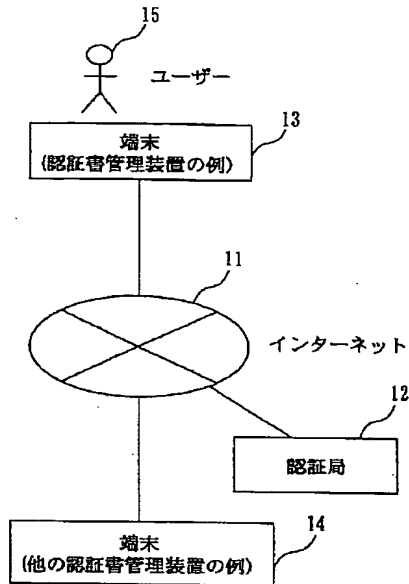
【図 12】 実施の形態 4 における端末の構成を示す図である。

【図 13】 実施の形態 4 における認証書管理部の処理フローを示す図である。

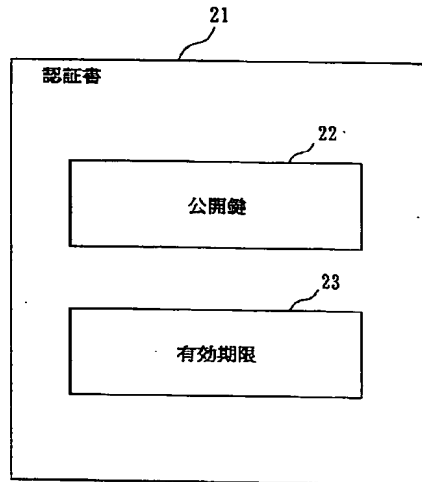
【符号の説明】

11 インターネット、12 認証局、13 端末、14 端末、15 ユーザー、21 認証書、22 公開鍵、23 有効期限、31 アプリケーション部、32 表示部、33 操作部、34 認証書管理部、35 更新期間判定部、36 更新催促情報出力部、37 更新指示入力部、38 認証書記憶部、39 日付・時刻管理部、40 更新要求出力部、41 秘密鍵記憶部、42 認証書受信部、43 認証書識別情報記憶部、51 認証書送信要否確認情報出力部、52 認証書送信指示部、53 認証書送信部、61 失効リスト更新日、62 失効リスト更新予定日、63 失効した認証書の認証書識別情報、64 失効した認証書の認証書識別情報、71 更新期間判定部、72 失効リスト記憶部、73 更新要求出力部、74 失効リスト受信部、81 更新催促情報出力部、82 更新指示入力部。

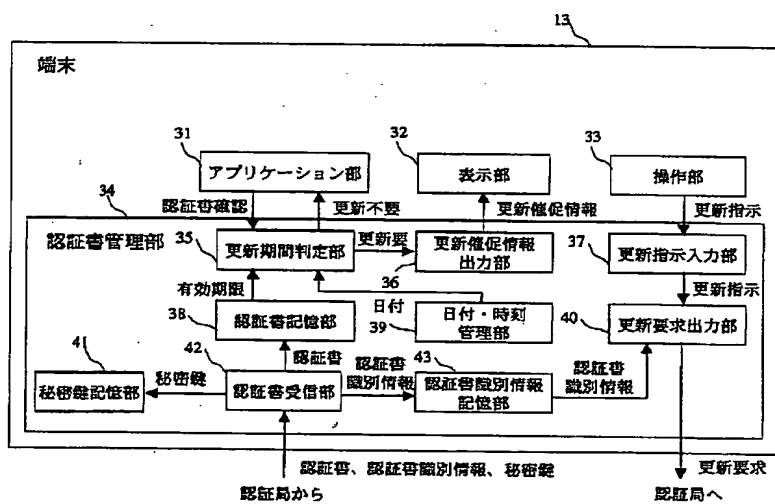
【図1】



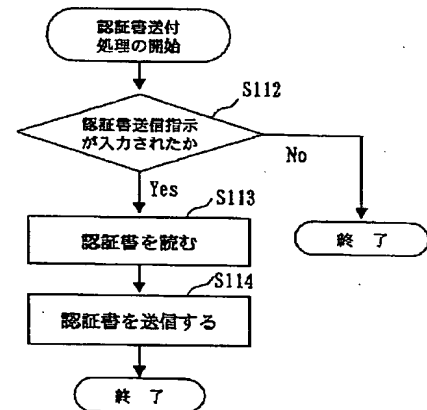
【図2】



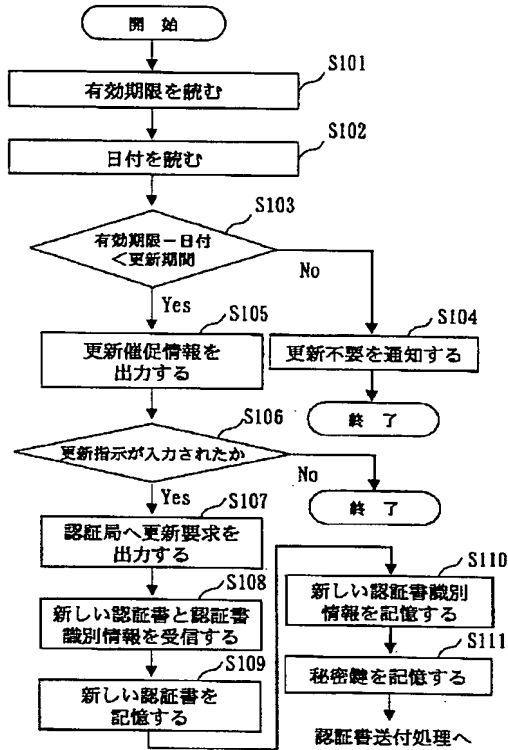
【図3】



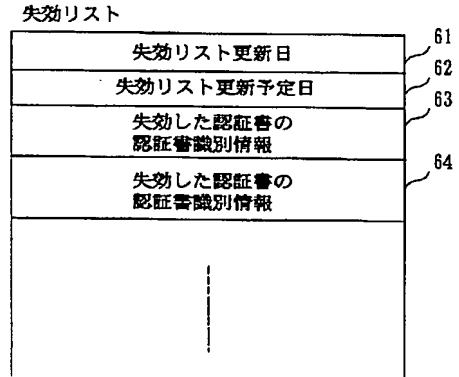
【図6】



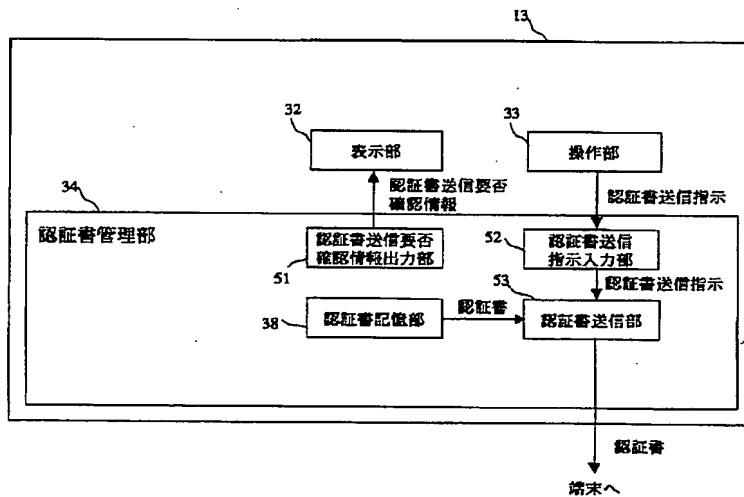
【図4】



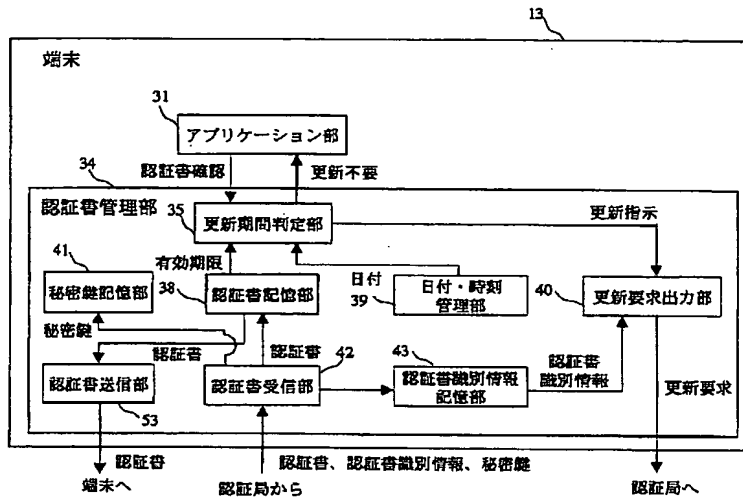
【図9】



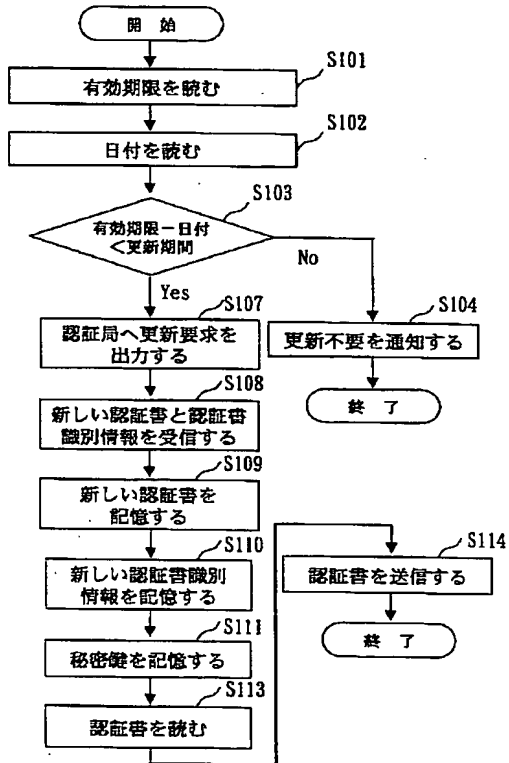
【図5】



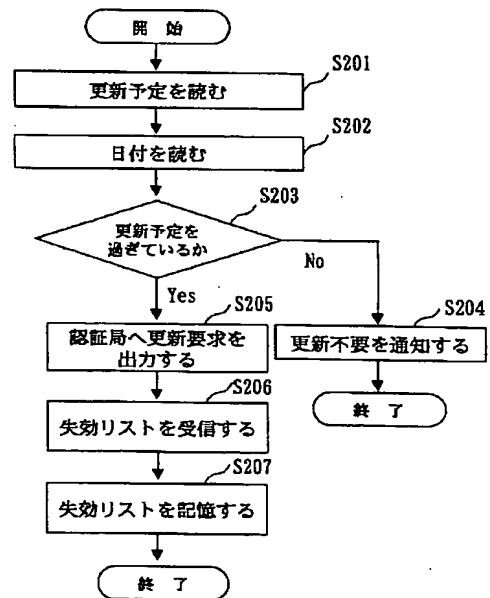
【図 7】



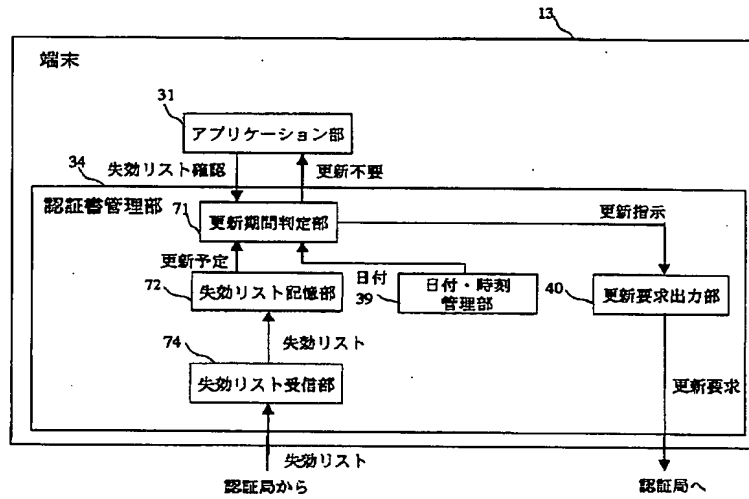
【図 8】



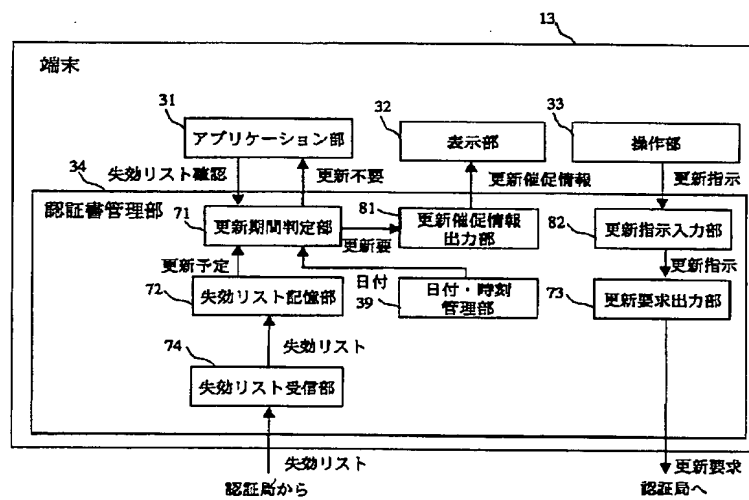
【図 1 1】



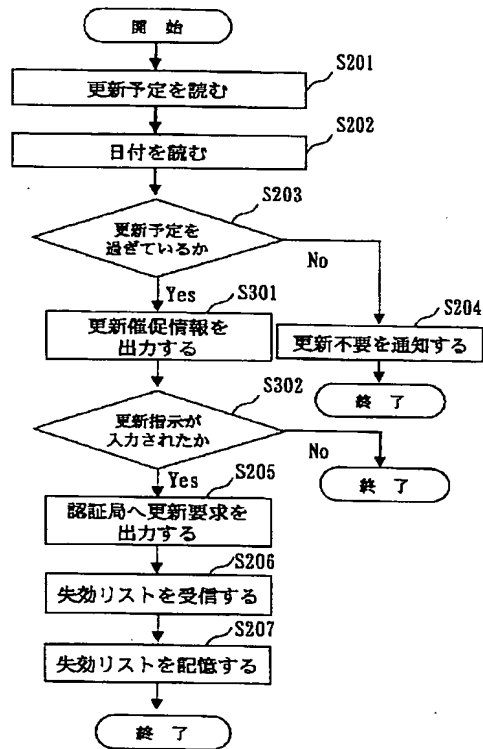
【図10】



【図12】



【図13】



フロントページの続き

Fターム(参考) 5B049 AA01 CC00 CC31 GG02 GG04
 5B089 GA21 GB02 HA10 JB22 KA17
 KB11
 5J104 AA07 AA11 KA01 KA05 MA02
 PA07

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

